International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(13s) 2026 pp. 742-757
https://doi.org/10.70917/ijcisim-2026-4118
Article

Geodefense-Based Defense Logistics Resilience Governance: An NVivo-Assisted Qualitative Inquiry in Jakarta

Ghazalie[1], Yusuf Ali[2], Aris Sarjito[3], Bambang Kustiawan[4], Tri Adianto[5]

[1,2,3,4] Doctoral Program in Defense Science, Universitas Pertahanan Republik Indonesia, Indonesia
[5] Department of Political Science, Faculty of Social and Political Sciences, UIN Sunan Gunung Djati Bandung, Indonesia
[1]ghazalie@doktoral.idu.ac.id,[2]yusufali8788@gmail.com, [3]arissarjito@gmail.com, [4]bkustiawan168@gmail.com,
[5]Corresponcence Email : tri.adianto@uinsgd.ac.id

Abstract: This article develops a geodefense-based defense logistics resilience governance framework for Jakarta, Indonesia, by foregrounding NVivo-assisted qualitative evidence from interviews, policy documents, and thematic visualization. The study responds to a central problem in contemporary urban defense management: strategic cities often possess extensive logistics and critical infrastructure capacity, yet their governance systems remain vulnerable to cascading disruption, fragmented policy authority, and weak civil-military integration. Using a qualitative case-study design, the research analyzes documentary and interview materials through NVivo 15 and interprets the resulting thematic structure through a systems-oriented policy lens. The NVivo coding matrix identified three analytical clusters: the condition of Jakarta's defense logistics infrastructure, the policy architecture governing that infrastructure, and the required geodefense-based policy model. The highest coded-reference nodes were field vulnerability, policy constraints, and functional integration, indicating that the core issue is not simply infrastructure scarcity but the absence of an integrated spatial-policy mechanism capable of transforming strategic civilian infrastructure into resilient defense logistics support during crises. The article proposes the Geodefense-Based Defense Logistics Resilience Governance (GDLR-G) framework, organized around five pillars: threat and vulnerability analysis, geodefense mapping through a Defense Infrastructure Mapping System, policy integration, geo-defense governance, and logistics readiness and response. The findings contribute to defense management, urban resilience, and critical infrastructure governance by showing how NVivo-supported thematic analysis can move beyond descriptive coding toward policy model construction for multidomain urban security environments.

Keywords: Geodefense; defense logistics; critical infrastructure; NVivo; urban resilience; civil-military coordination; Jakarta; defense governance

1. Introduction

Urban defense management has become a central problem for states facing hybrid, cyber, ecological, and infrastructure-based disruptions. Contemporary threats increasingly target the functions that allow the state to govern, mobilize, communicate, and sustain public order. Ports, airports, energy facilities, data centers, telecommunications networks, roads, rail systems, and water infrastructure are no longer peripheral assets that merely support economic activity; they are strategic systems whose interruption can weaken national resilience, reduce military mobility, and disrupt crisis response. In this environment, the security of a capital city cannot be understood only through conventional territorial defense. It must be analyzed as a system of interdependent logistics, spatial, institutional, and digital infrastructures that jointly determine whether the state can continue to function during a crisis (Hoffman, 2007; Kaldor, 2012; NATO, 2022; Cybersecurity and Infrastructure Security Agency, 2019).

Jakarta provides a particularly important case for this problem. The city has long operated as Indonesia's political, administrative, economic, diplomatic, and logistics center. Its infrastructure connects government institutions, ports, airports, energy distribution, mass transportation, financial services, public communication, and emergency response systems. This concentration generates operational capacity in normal conditions, but it also

creates systemic exposure. When strategic infrastructures are densely concentrated and highly interdependent, a disruption in one node can create cascading effects across other sectors. The problem is therefore not reducible to whether Jakarta has infrastructure, but whether that infrastructure is governed as a resilient defense logistics system (Ministry of Defence of the Republic of Indonesia, 2015; OECD, 2019; UN-Habitat, 2022).

The article addresses this issue by developing a geodefense-based defense logistics resilience governance framework. Geodefense is used here as a spatial-defense approach that links geography, infrastructure, logistics corridors, threat exposure, and institutional decision making. It emphasizes the location of critical nodes, the vulnerability of strategic corridors, the existence of single points of failure, the availability of redundancy, and the capacity of state and non-state actors to coordinate under stress. A geodefense perspective is especially relevant in strategic urban environments because the meaning of infrastructure is inseparable from its location, connectivity, and function within a wider system (Clausewitz, 1976; Graham, 2010; Linkov & Trump, 2019).

The study is grounded in a qualitative inquiry that used NVivo 15 to support data organization, coding, thematic mapping, and visualization. The NVivo findings are not treated as a mechanical output. Rather, they serve as an audit trail and analytic bridge between qualitative evidence and model development. This is important because qualitative policy research often faces criticism when it moves from interview findings to a proposed model without making the analytic pathway explicit. By foregrounding NVivo coding, word-frequency patterns, thematic hierarchy, and project-map interpretation, this article demonstrates how qualitative data can support a structured governance framework (Allsop et al., 2022; Bazeley & Jackson, 2013; Silver & Lewins, 2014).

The central research question is: How can NVivo-assisted qualitative evidence inform a geodefense-based defense logistics resilience governance model for Jakarta? This question is supported by three subsidiary questions. First, what conditions and vulnerabilities characterize Jakarta's defense logistics infrastructure? Second, what policy and governance gaps shape the use of strategic urban infrastructure for defense logistics purposes? Third, what integrated model can connect spatial analysis, policy alignment, actor coordination, and logistics readiness into a usable governance framework?

The article makes three contributions. Theoretically, it connects urban resilience, critical infrastructure protection, defense logistics, and geodefense into a single governance logic. Methodologically, it shows how NVivo-assisted analysis can strengthen transparency in qualitative defense policy research by linking coding results to model construction. Practically, it proposes a five-pillar framework for transforming Jakarta from a policy-rich but system-poor infrastructure environment into an urban strategic defense node with more integrated resilience governance (Braun & Clarke, 2006; Creswell & Poth, 2018; OECD, 2019).

2. Literature Review and Conceptual Background

The first conceptual foundation of the study is critical infrastructure resilience. Infrastructure resilience refers to the capacity of infrastructure systems to anticipate, absorb, adapt to, recover from, and learn from disruption. In a strategic city, resilience is not limited to physical hardening. It also includes redundancy, interoperability, decision speed, continuity of operations, multi-actor coordination, and the ability to preserve essential services during stress. Critical infrastructure literature emphasizes that modern infrastructures operate as interdependent systems. Energy enables telecommunications, telecommunications support transport management, transport supports logistics, and logistics supports defense mobility and public survival. This means that resilience must be assessed across networks rather than only at the level of isolated facilities (Amin, 2002; Holling, 1973; Linkov & Trump, 2019; OECD, 2019; Rodin, 2014).

The second foundation is urban resilience. A city is not merely a bounded administrative space but a complex system of systems. It consists of technical networks, public institutions, social activity, economic flows, mobility patterns, and spatial arrangements. Urban resilience scholarship stresses that dense cities may be efficient in normal times but fragile under shock when interdependencies are unmanaged. Jakarta's strategic relevance therefore lies not only in its size, but in the way its logistics and governance systems connect the local, metropolitan, national, and defense scales. Urban resilience offers the vocabulary of cascading effects, adaptive capacity, redundancy, and recovery, while defense management adds the requirements of mobilization, prioritization, and national security continuity (Ackoff, 1971; Graham & Marvin, 2001; Meerow et al., 2016; UN-Habitat, 2022).

The third foundation is defense logistics. Defense logistics concerns the planning, movement, storage, distribution, maintenance, and protection of resources necessary to sustain defense operations. In multidomain conflict and crisis environments, logistics is not simply an internal military function. It depends heavily on civilian

transportation networks, commercial operators, telecommunications, fuel distribution, energy resilience, cyber-secure data systems, and local authority coordination. The concept of dual-use infrastructure is therefore essential. Roads, ports, airports, rail systems, depots, data networks, and emergency facilities may serve civilian functions in normal periods but become decisive for defense logistics in contingencies. A city such as Jakarta requires policies that identify when and how civilian infrastructure can be prioritized for defense-related continuity without paralyzing public services (Alberts & Hayes, 2003; European Commission, 2022; Government of Indonesia, 2002, 2019, 2021; NATO, 2024; U.S. Department of Defense, 2022).

The fourth foundation is collaborative governance. Infrastructure and logistics governance in a strategic city involves ministries, local government, military and police institutions, state-owned enterprises, private infrastructure operators, telecommunications providers, emergency agencies, cyber authorities, and communities. No single organization controls all required assets. Collaborative governance provides a framework for understanding how such actors can coordinate through shared rules, trust, joint forums, information exchange, and agreed operational protocols. For defense logistics resilience, collaboration must be more than informal coordination. It has to be institutionalized into policy alignment, data sharing, joint exercises, and emergency priority mechanisms (Ansell & Gash, 2008; Head & Alford, 2015; OECD, 2019).

The fifth foundation is geodefense. Although the term is less established than urban resilience or critical infrastructure protection, its underlying logic is consistent with geostrategy, geospatial intelligence, territorial defense, and infrastructure risk analysis. Geodefense treats space as a strategic variable. The value and vulnerability of infrastructure depend on its location, access, interconnections, proximity to hazards, role in logistics flows, and relation to other critical nodes. In the Jakarta case, a geodefense approach means mapping ports, airports, logistics corridors, energy nodes, data infrastructure, government centers, transport chokepoints, evacuation routes, and alternative routes as part of a defense logistics system (Clausewitz, 1976; Graham, 2010; Kilcullen, 2013).

This article integrates these literatures through the concept of Geodefense-Based Defense Logistics Resilience Governance (GDLR-G). GDLR-G refers to a governance arrangement that uses spatial-defense analysis to align infrastructure policy, critical-node mapping, civil-military coordination, and logistics readiness. It assumes that the key vulnerability in strategic cities is not only material exposure but governance fragmentation. A city may possess major infrastructure assets but still fail to operate as a resilient defense logistics system if policies remain sectoral, actors lack interoperable procedures, data are not integrated, and priority mechanisms are unclear during emergencies (Head, 2023; Rittel & Webber, 1973; Linkov & Trump, 2019).

The conceptual position of this article is therefore that defense logistics resilience is produced by the interaction of four dimensions: spatial intelligence, infrastructure functionality, policy integration, and operational readiness. Spatial intelligence identifies where critical nodes and corridors are located. Infrastructure functionality clarifies what those nodes do and how they support state continuity. Policy integration aligns the authority and rules needed to use those assets. Operational readiness turns the model into tested procedures through drills, redundancy plans, and crisis decision protocols (Checkland, 1981; Checkland & Scholes, 1990; Cybersecurity and Infrastructure Security Agency, 2024; OECD, 2019).

3. Methodology

The study uses a qualitative case-study design focused on Jakarta as a strategic urban defense logistics environment. A qualitative approach is appropriate because the research problem concerns institutional meaning, actor perception, policy fragmentation, and systemic vulnerability rather than only measurable infrastructure capacity. The analytical objective is not to estimate a statistical relationship, but to interpret how knowledgeable actors and policy documents construct the problem of defense logistics infrastructure and how those interpretations can inform a governance model (Creswell & Poth, 2018; Moustakas, 1994; Patton, 2015).

The empirical materials consisted of interview transcripts, focus group or round table discussion materials, policy documents, and supporting contextual observations. The documentary corpus included spatial planning documents, development planning materials, defense-related regulations, critical infrastructure references, and sectoral policy documents relevant to transportation, energy, communication, disaster response, and security. Interview sources represented policy, operational, academic, and infrastructure-management perspectives. The use of multiple sources enabled methodological triangulation and allowed the analysis to compare formal policy narratives with the concerns expressed by actors involved in infrastructure, defense, and crisis governance (Bowen, 2009; Denzin, 2012; Lincoln & Guba, 1985).

Table 1. Qualitative data sources and NVivo-supported analytical functions

Data source	Analytical role	NVivo function
Interview transcripts	Capture actor perceptions on vulnerability, coordination, policy gaps, and model needs	Source classification, open coding, node retrieval
FGD/RTD materials	Identify shared and contested meanings across stakeholder groups	Thematic comparison and memoing
Policy and planning documents	Assess formal rules, spatial planning, development priorities, and defense-related mandates	Document coding and matrix comparison
Observation/contextual notes	Support interpretation of urban infrastructure condition and institutional context	Analytic memoing and triangulation

Source: Processed by the author using NVivo 15, 2026.

NVivo 15 was used to organize, code, query, and visualize the qualitative materials. The analytic process followed three broad stages. First, the materials were imported, classified, and organized by source type. Second, open and axial coding were used to identify recurring concepts related to infrastructure condition, policy governance, and model requirements. Third, selective coding and thematic interpretation consolidated the codes into a hierarchical structure connected to the study's three analytical questions. NVivo supported transparency by making it possible to trace a theme back to coded sources and references (Bazeley & Jackson, 2013; Saldaña, 2021; Silver & Lewins, 2014).

The analysis distinguished between the technical function of NVivo and the interpretive responsibility of the researcher. NVivo did not generate the findings automatically. It supported data management, coding consistency, source retrieval, project mapping, hierarchy charts, and word-frequency visualization. The meaning of each node was interpreted through the theoretical lens of geodefense, critical infrastructure resilience, collaborative governance, and defense logistics. This distinction is important because computer-assisted qualitative data analysis software increases traceability but does not replace conceptual judgment (Allsop et al., 2022; Silver & Lewins, 2014; Strauss & Corbin, 1998).

The coding structure was organized into three parent clusters. The first cluster concerned the condition of Jakarta's defense logistics infrastructure and included operational function, strategic infrastructure, system capacity, field vulnerability, and operational readiness. The second cluster concerned policy and governance and included civil-military integration, policy constraints, actor coordination, infrastructure utilization, and emergency prioritization. The third cluster concerned the required model and included priority facilities, geodefense, functional integration, integrated coordination, and readiness exercises. The use of this structure allowed the research to move from diagnosis, to policy interpretation, to model construction (Braun & Clarke, 2006, 2021; Saldaña, 2021).

To avoid overstating the numerical meaning of qualitative coding, the article treats coded-reference counts as indicators of thematic salience rather than as statistical measurements. A high number of coded references suggests that a theme appeared frequently and substantively across the dataset; it does not prove causal weight in a quantitative sense. The analysis therefore combines coded-reference patterns with interpretive reading of the content and relationships among themes. This approach is consistent with qualitative validity standards that emphasize credibility, triangulation, thick interpretation, auditability, and coherence between data and claims (Lincoln & Guba, 1985; Miles et al., 2014; Patton, 2015).

4. Results: NVivo-Assisted Thematic Findings

The NVivo results show a coherent thematic architecture across the data. The parent theme is the need for a geodefense-based model of defense logistics infrastructure policy in Jakarta. Under this parent theme, three major clusters emerged. The first cluster describes the strategic but vulnerable condition of Jakarta's infrastructure. The second cluster identifies policy constraints and governance fragmentation. The third cluster identifies the model requirements needed to integrate spatial analysis, policy alignment, and logistics readiness. The pattern is analytically

important because it shows a progression from problem condition to governance gap and then to model construction (Braun & Clarke, 2021; Saldaña, 2021).

The coding matrix indicates that field vulnerability, policy constraints, and functional integration were the most salient nodes in the dataset. Field vulnerability and policy constraints each recorded 48 coded references, while functional integration recorded 47 coded references. This pattern suggests that the central issue is not merely whether infrastructure exists, but how vulnerabilities and governance constraints prevent infrastructure from operating as a resilient defense logistics system. The result also indicates that the proposed model must prioritize integration rather than simple asset expansion (Bazeley & Jackson, 2013; Miles et al., 2014; Silver & Lewins, 2014).

Table 2. NVivo thematic coding matrix derived from the dissertation coding output. Source: Processed by the author using NVivo 15, 2026.

Cluster	Thematic node	Sources coded	Coded references
Condition	Field vulnerability	24	48
Condition	Operational readiness	16	27
Condition	Strategic infrastructure	16	21
Condition	Operational function	17	20
Condition	System capacity	12	17
Policy	Policy constraints	25	48
Policy	Emergency prioritization	18	25
Policy	Actor coordination	16	21
Policy	Civil-military integration	16	20
Policy	Infrastructure utilization	9	10
Model	Functional integration	26	47
Model	Integrated coordination	19	29
Model	Geodefense	20	27
Model	Priority facilities	9	13
Model	Readiness exercises	10	11

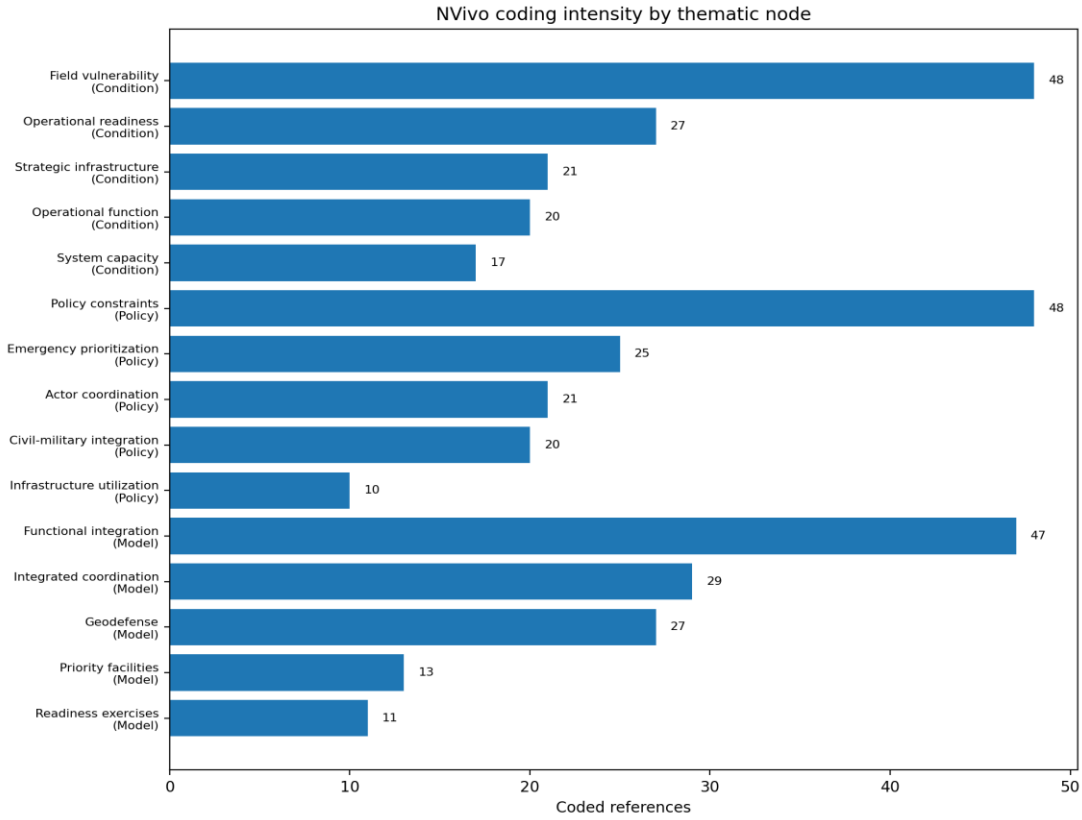

Figure 1. NVivo coding intensity by thematic node. Values are coded references from the NVivo output, interpreted as thematic salience rather than statistical frequency. Source: Processed by the author using NVivo 15, 2026.

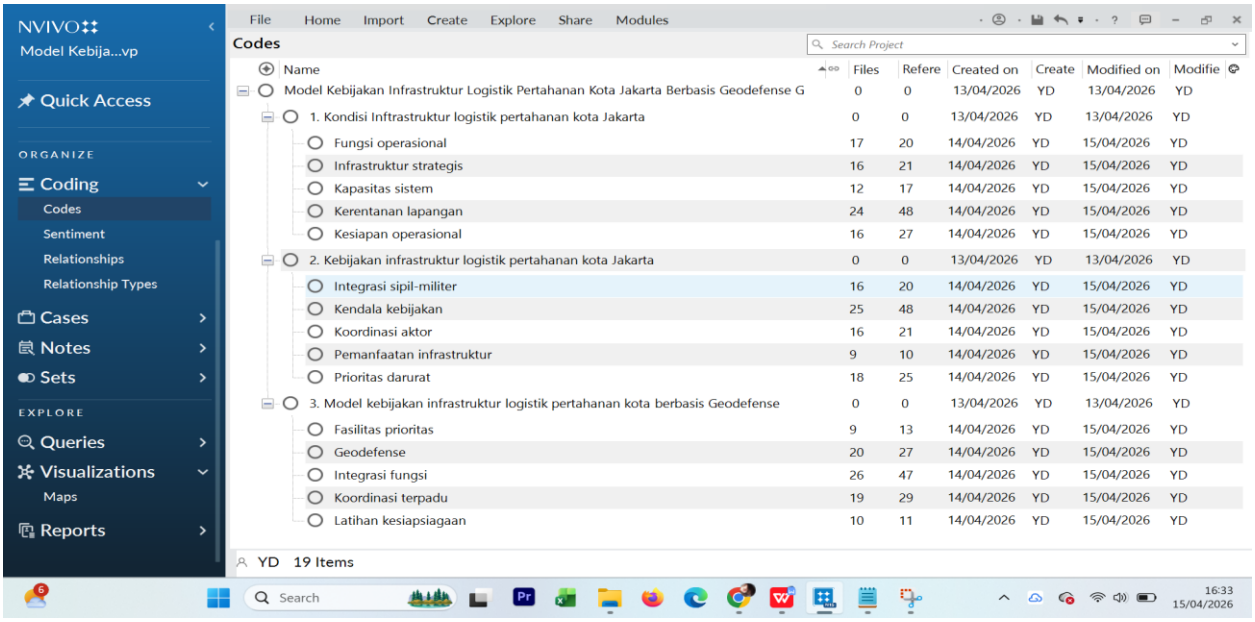

Figure 2. NVivo coding matrix screenshot showing the three parent clusters and child-node reference counts. Source: Author's NVivo project output, 2026.

In the first cluster, field vulnerability was the most dominant theme, followed by operational readiness, strategic infrastructure, operational function, and system capacity. This means that informants and documents recognized

Jakarta's infrastructure as strategically valuable, but their attention concentrated on exposure, chokepoints, operational uncertainty, and the risks created by dense interdependence. Strategic infrastructure such as ports, roads, transport nodes, energy facilities, and communication systems can support defense logistics, yet they are also vulnerable to congestion, physical disruption, cyber disruption, ecological hazards, and coordination delays (Amin, 2002; Cybersecurity and Infrastructure Security Agency, 2019; Linkov & Trump, 2019).

The node for operational readiness is also significant. It shows that the ability to use infrastructure during a crisis depends not only on physical capacity but on preparedness, procedures, exercises, and decision authority. A facility may be large or technically advanced, but it will not necessarily function as a defense logistics asset unless its crisis role has been anticipated. This distinction between capacity and readiness is one of the most important findings. Jakarta can be described as strong in capacity but weak in integrated resilience, because its strategic assets are not yet fully embedded in a geodefense-based crisis governance system (NATO, 2024; OECD, 2019; United Nations Office for Disaster Risk Reduction, 2015).

In the second cluster, policy constraints were the most prominent node, followed by emergency prioritization, actor coordination, civil-military integration, and infrastructure utilization. This indicates that the policy challenge is less about the absence of regulations and more about the fragmentation of authority, planning, and operational rules. Multiple documents and institutions exist, but they do not yet produce a single integrated governance system for defense logistics resilience. The phrase policy-rich but system-poor captures this finding: the policy environment contains many sectoral instruments, yet lacks an integrated spatial-defense mechanism (Ansell & Gash, 2008; Head & Alford, 2015; Ministry of Defence of the Republic of Indonesia, 2015).

Emergency prioritization emerged as a substantial policy theme. Informants and documents pointed toward the need to define which facilities, routes, actors, and functions should receive priority during crisis conditions. Without a priority mechanism, strategic infrastructure may be contested by routine civilian use, emergency public service demand, and defense logistics needs at the same time. This creates the risk of delay when rapid mobilization is required. A geodefense governance model must therefore include rules for prioritizing critical corridors, alternative routes, energy supply, communication access, data integrity, and logistics nodes under different threat scenarios (European Commission, 2022; NATO, 2024; U.S. Department of Defense, 2022).

Civil-military integration and actor coordination are closely related but not identical. Civil-military integration concerns the alignment of civilian infrastructure functions with defense needs. Actor coordination concerns the process by which ministries, local government, the military, the police, state-owned enterprises, private operators, cyber authorities, and emergency agencies share information and make decisions. The NVivo results suggest that both are necessary. Civilian infrastructure cannot support defense logistics simply because it exists; actors must agree on access, authority, command relationships, data flows, and operational triggers before a crisis occurs (Government of Indonesia, 2002, 2019, 2021; OECD, 2019).

In the third cluster, functional integration was the highest node, followed by integrated coordination and geodefense. This confirms that the model expected by the data is not a narrow technical map or a conventional coordination forum. It is a governance framework that integrates the civilian, logistics, defense, spatial, and emergency functions of infrastructure. Functional integration means that infrastructure is evaluated based on how it can support multiple functions across normal, alert, emergency, and recovery phases. Geodefense then provides the spatial logic for determining which nodes matter most, where vulnerabilities are concentrated, and how redundancy should be built (Checkland, 1981; Checkland & Scholes, 1990; Linkov & Trump, 2019).

The word-frequency visualization supports the thematic structure. Dominant words included logistics, infrastructure, defense, policy, Jakarta, geodefense, development, national, strategic, threat, coordination, vulnerability, and resilience-related terms. This confirms that the empirical narrative was centered on the relationship between strategic infrastructure, defense governance, and spatially informed policy. However, word clouds must be read carefully because procedural words from interview templates may appear alongside substantive terms. The analytic value of the word-frequency result lies in its function as an initial orientation, not as a standalone finding (Braun & Clarke, 2006; Bazeley & Jackson, 2013; Silver & Lewins, 2014).

Figure 3. NVivo word-frequency visualization. Source: Author's NVivo project output, 2026.

The hierarchy and treemap visualizations further confirmed that the three clusters were relatively balanced but internally differentiated. In the condition cluster, field vulnerability dominated. In the policy cluster, policy constraints and emergency prioritization dominated. In the model cluster, functional integration dominated. This creates a clear explanatory chain: Jakarta has strategically important infrastructure that remains vulnerable; vulnerability is intensified by policy constraints and weak emergency priority systems; therefore, the required model must integrate functions through a geodefense-based governance mechanism (Miles et al., 2014; Saldaña, 2021).

The final NVivo project-map interpretation showed dense connections between sources and nodes. Many sources were linked to more than one cluster, indicating that informants did not discuss infrastructure condition, policy governance, and model requirements as separate domains. A single statement could relate to field vulnerability, actor coordination, emergency prioritization, and geodefense mapping. This pattern supports the classification of the problem as systemic. It is not a linear infrastructure problem that can be solved through a single agency or a single regulation. It is a multi-actor policy system requiring integrated analysis and coordinated implementation (Ackoff, 1971; Checkland, 1981; Head, 2023).

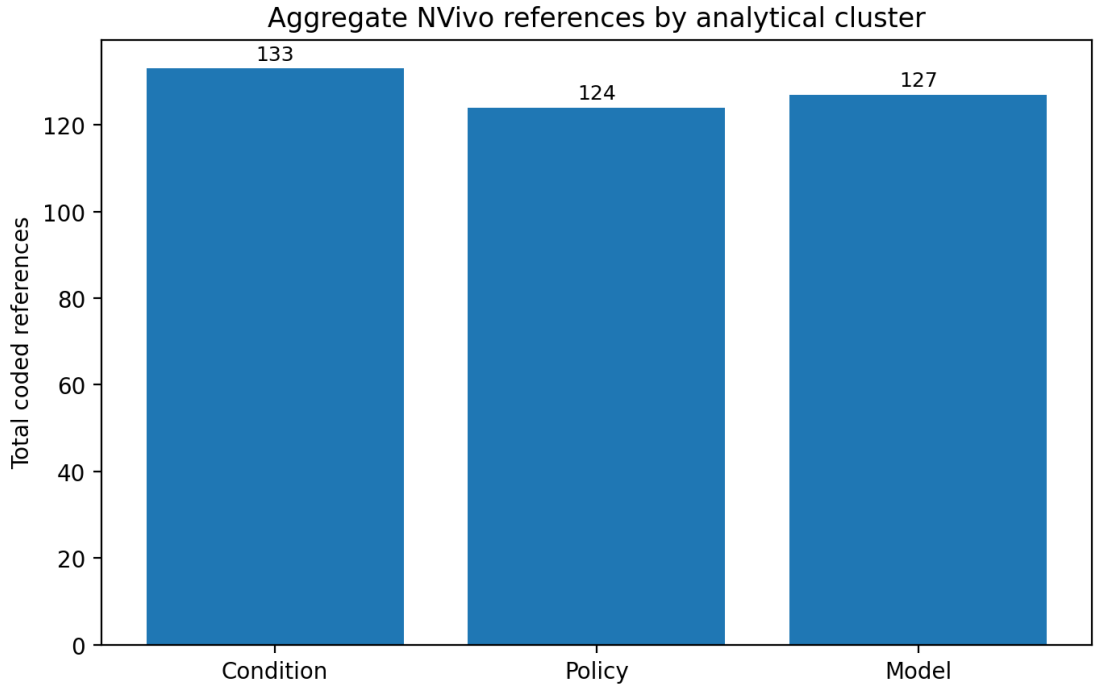

Figure 4. Aggregate NVivo references by analytical cluster. Values are summed from the child-node reference counts in Table 2. Source: Processed by the author using NVivo 15, 2026.

Based on the coding pattern, the study formulates the GDLR-G framework. The framework has five pillars. The first pillar is threat and vulnerability analysis, which identifies multidomain threats, field vulnerabilities, critical nodes, critical corridors, and single points of failure. The second pillar is geodefense mapping through a Defense Infrastructure Mapping System, which turns infrastructure data into spatially usable decision support. The third pillar is policy integration, which aligns spatial planning, development planning, defense policy, and sectoral infrastructure rules. The fourth pillar is geo-defense governance, which institutionalizes multi-actor coordination. The fifth pillar is logistics readiness and response, which translates the model into early warning, mobilization, redundancy, and recovery mechanisms (Checkland & Scholes, 1990; Linkov & Trump, 2019; OECD, 2019).

The findings show that GDLR-G is not simply a conceptual label. It is derived from the observed relationship among the highest-salience NVivo nodes. Field vulnerability generates the need for threat and vulnerability analysis. Policy constraints generate the need for policy integration. Functional integration generates the need for geodefense-based governance. Emergency prioritization generates the need for readiness procedures. Actor coordination and civil-military integration generate the need for a formal governance mechanism. In this way, the model is empirically grounded in the NVivo-assisted qualitative evidence (Braun & Clarke, 2021; Lincoln & Guba, 1985; Saldaña, 2021).

Table 3. Core NVivo findings and governance implications

Dominant NVivo evidence	Interpretation	Governance implication
Field vulnerability (48 references)	Strategic infrastructure is exposed to congestion, hazard, disruption, and interdependence risks	Create threat and vulnerability analysis linked to critical nodes and corridors
Policy constraints (48 references)	The problem is not the absence of policy, but weak integration and operationalization	Build a policy alignment matrix across planning, infrastructure, and defense domains
Functional integration (47 references)	The preferred model must connect civilian, logistics, defense, and emergency functions	Institutionalize geodefense governance and dual-use infrastructure mechanisms
Emergency prioritization (25 references)	Crisis conditions require pre-agreed decisions on routes, facilities, and authority	Develop priority protocols and scenario-based readiness exercises

Source: Processed by the author using NVivo 15, 2026.

The result can also be expressed as a transformation logic. The current condition is characterized by strategic infrastructure capacity, high interdependence, field vulnerability, fragmented policy, and limited emergency prioritization. The desired condition is an urban strategic defense node in which critical infrastructure is mapped, prioritized, protected, coordinated, and exercised as part of a broader defense logistics resilience system. GDLR-G is the proposed bridge between these two conditions (Holling, 1973; Linkov & Trump, 2019; OECD, 2019).

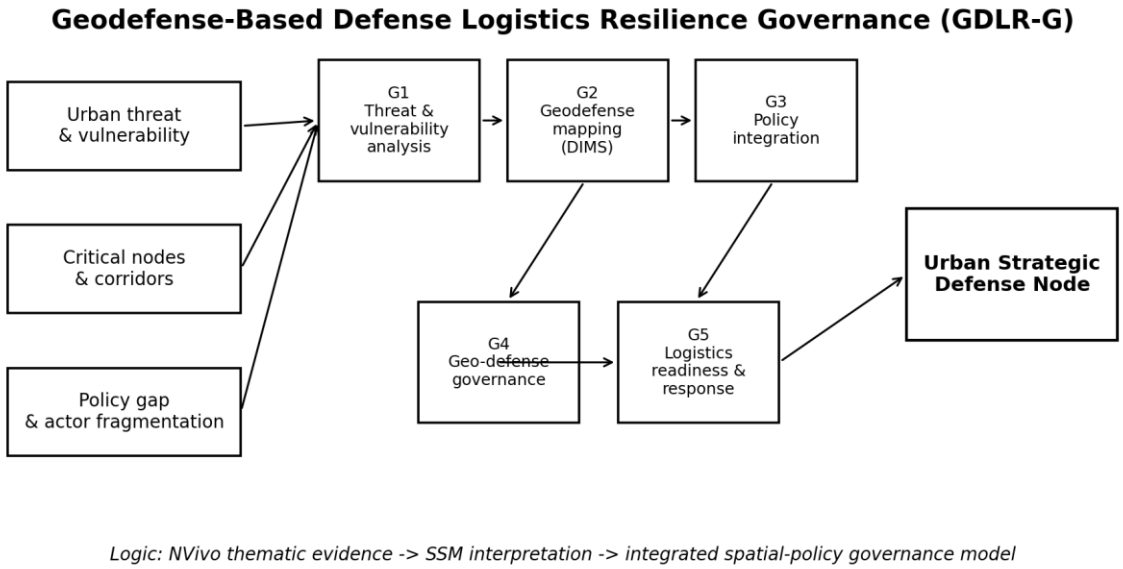

Figure 5. Proposed GDLR-G framework derived from NVivo-assisted thematic findings and systems interpretation. Source: Processed by the author using NVivo 15, 2026.

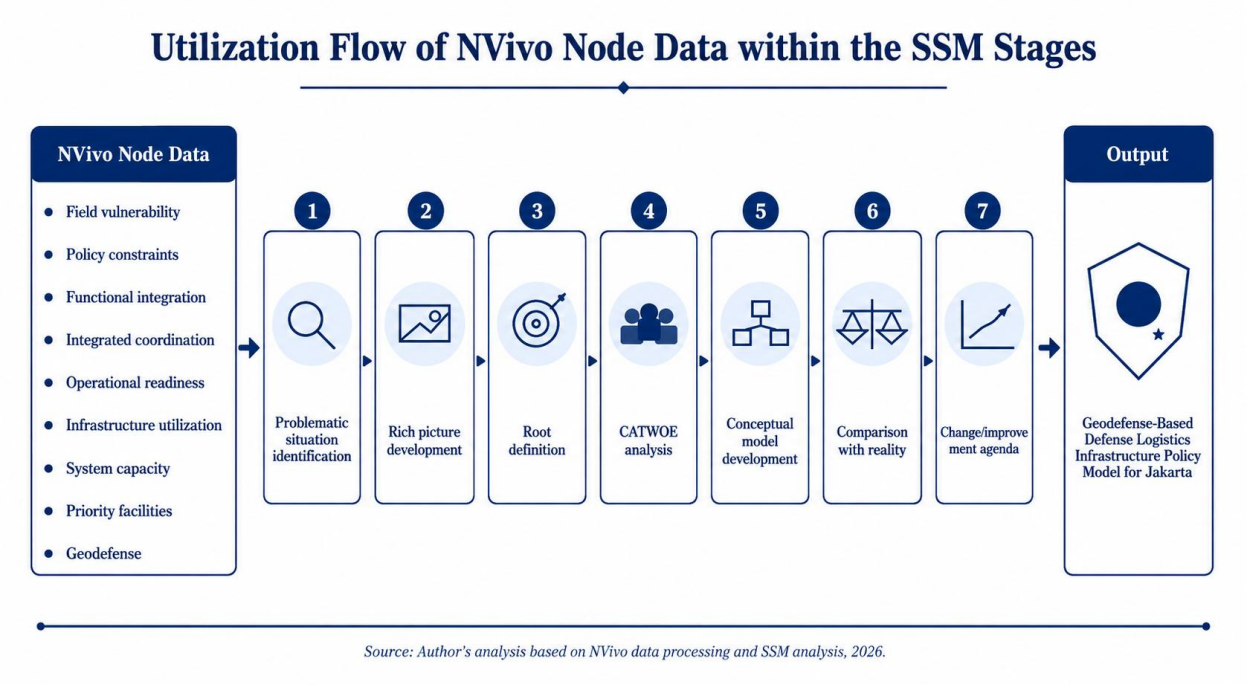

Figure 6. NVivo-to-SSM analytical transition used in the doctoral study. Source: Author's synthesis based on NVivo and SSM analysis, 2026.

Table 4. Five pillars of the GDLR-G framework. Source: Processed by the author using NVivo 15, 2026.

Pillar	Core function	Operational output

G1. Threat and vulnerability analysis	Identify multidomain threats, field vulnerabilities, critical nodes, critical corridors, and single points of failure	Threat-vulnerability profile and criticality register
G2. Geodefense mapping	Convert infrastructure and vulnerability information into spatial decision support	Defense Infrastructure Mapping System (DIMS)
G3. Policy integration	Align spatial planning, development planning, sectoral infrastructure policy, and defense policy	Policy alignment matrix and integrated planning checklist
G4. Geo-defense governance	Institutionalize civil-military and multi-actor coordination	Permanent coordination forum, data-sharing protocol, and joint command triggers
G5. Logistics readiness and response	Translate governance into early warning, mobilization, redundancy, and recovery procedures	Crisis SOPs, exercise program, and continuity-of-operations plan

5. Discussion

The results have several implications for defense management and urban governance. First, the findings challenge an infrastructure-centric view of logistics resilience. It is common for policy discussions to focus on the physical adequacy of ports, roads, depots, power systems, or communication facilities. This study shows that physical capacity is only one layer of resilience. A city may have extensive infrastructure but still remain vulnerable if those assets are not integrated into a spatially informed governance system. For Jakarta, the issue is not simply the presence of infrastructure; it is the ability to govern infrastructure as a defense logistics system under stress (Cybersecurity and Infrastructure Security Agency, 2019; OECD, 2019; Rodin, 2014).

Second, the findings reinforce the importance of policy integration. The NVivo results show that policy constraints were among the most salient themes. This indicates that regulations, planning documents, and sectoral mandates may exist without producing operational coherence. In a strategic city, sectoral policy can become a source of vulnerability when each institution manages its own assets without a shared defense logistics perspective. Policy integration therefore needs to move beyond document harmonization. It should include shared indicators, joint planning cycles, interoperable data systems, agreed emergency priorities, and exercise-based evaluation (Ansell & Gash, 2008; Head & Alford, 2015; OECD, 2019).

Third, the study demonstrates the practical value of geodefense. Spatial analysis is often discussed in relation to mapping or geographic information systems, but the geodefense approach used here is broader. It connects spatial location with strategic function, vulnerability, governance authority, and logistics prioritization. A port, road corridor, energy substation, or data facility becomes important not only because of what it is, but because of where it is, what it connects, what depends on it, and what happens if it fails. This perspective supports more precise decisions about facility prioritization, redundancy investment, and crisis routing (Clausewitz, 1976; Graham, 2010; Kilcullen, 2013).

Fourth, the findings show that civil-military integration should be institutionalized before crisis conditions occur. In a large urban system, improvised coordination may not be sufficient. A severe disruption can produce simultaneous demands from public services, commercial logistics, emergency response, and defense mobilization. If authority, priorities, and access rules are unclear, the state may lose time during the decisive early phase of crisis response. GDLR-G therefore proposes geo-defense governance as a standing mechanism rather than an ad hoc meeting structure. It should include data sharing, joint planning, scenario exercises, and agreed protocols for infrastructure utilization (Alberts & Hayes, 2003; European Commission, 2022; NATO, 2024).

Fifth, the results offer a methodological contribution. NVivo-assisted qualitative analysis can support policy model construction when the researcher uses coding not merely to classify data but to build a transparent chain from evidence to concept. In this article, coded-reference patterns identified the most salient issues, word-frequency analysis oriented the thematic landscape, hierarchy charts clarified the distribution of nodes, and project maps showed cross-node relationships. These outputs then informed the five-pillar GDLR-G framework. The process demonstrates how computer-assisted qualitative analysis can strengthen auditability in complex defense policy studies (Allsop et al., 2022; Bazeley & Jackson, 2013; Silver & Lewins, 2014).

Nevertheless, the approach has limitations. NVivo coding counts should not be interpreted as statistical proof. A high coded-reference count indicates salience in the qualitative corpus, not population-level frequency or causal magnitude. The analysis also depends on the quality of coding decisions, source selection, interview depth, and researcher interpretation. Further research should complement this qualitative model with geospatial risk scoring, network analysis, logistics simulation, multi-criteria decision analysis, or structural equation modeling to measure the relationships suggested by the qualitative findings (Lincoln & Guba, 1985; Miles et al., 2014; Patton, 2015).

The Jakarta case also has comparative relevance. Many capitals and metropolitan regions in Southeast Asia and beyond face similar problems: dense population, concentrated infrastructure, high dependence on digital systems, exposure to flooding or climate hazards, and fragmented governance. The GDLR-G framework can be adapted to other strategic cities by replacing the empirical inventory of nodes, corridors, policies, and actors. Its logic is portable, but its implementation must be locally grounded. Each city has different geography, institutional capacity, threat exposure, and infrastructure networks (Graham & Marvin, 2001; Meerow et al., 2016; UN-Habitat, 2022; United Nations Office for Disaster Risk Reduction, 2015).

The broader implication is that urban defense resilience requires a shift from asset protection to system governance. Asset protection asks how to secure individual facilities. System governance asks how infrastructure networks, actors, policies, and spatial priorities can continue to function when conditions deteriorate. For Jakarta, this shift is essential because the city's strategic value is generated by the interconnectedness of its systems. The same interconnectedness also creates risk. Geodefense-based governance is therefore a way to convert interdependence from a source of fragility into a source of coordinated resilience (Amin, 2002; Holling, 1973; Linkov & Trump, 2019).

6. Conclusion

This article developed a geodefense-based defense logistics resilience governance framework through NVivo-assisted qualitative inquiry in Jakarta. The findings show that Jakarta's defense logistics infrastructure is strategically significant but systemically vulnerable. The dominant NVivo nodes were field vulnerability, policy constraints, and functional integration. These themes reveal that the central problem is not a simple shortage of infrastructure. Rather, it is the absence of an integrated spatial-policy governance mechanism capable of converting civilian strategic infrastructure into resilient defense logistics support during crisis conditions (Braun & Clarke, 2021; Saldaña, 2021).

The study concludes that Jakarta can be characterized as strong in infrastructure capacity but weak in integrated resilience. It is also policy-rich but system-poor. Strategic infrastructure exists, and multiple policies regulate planning, development, security, and emergency functions. However, the link among spatial planning, defense policy, infrastructure governance, and civil-military coordination remains insufficiently institutionalized. This creates exposure to single points of failure, unclear emergency priorities, delayed coordination, and limited readiness for multidomain disruption (OECD, 2019; Ministry of Defence of the Republic of Indonesia, 2015).

The proposed GDLR-G framework responds to these gaps through five pillars: threat and vulnerability analysis, geodefense mapping, policy integration, geo-defense governance, and logistics readiness and response. The framework positions Jakarta as a potential urban strategic defense node where infrastructure is not merely protected as an asset but governed as part of a dynamic logistics resilience system. The model emphasizes critical-node identification, Defense Infrastructure Mapping System development, policy alignment matrices, standing civil-military coordination mechanisms, and readiness exercises across normal, alert, emergency, and recovery phases (Checkland, 1981; Checkland & Scholes, 1990; Cybersecurity and Infrastructure Security Agency, 2024).

The study contributes to scholarship by integrating geodefense, urban resilience, critical infrastructure governance, and defense logistics into a single conceptual framework. It contributes methodologically by demonstrating how NVivo-supported qualitative analysis can strengthen transparency in moving from empirical coding to policy model formulation. It contributes practically by offering a governance framework that can inform defense planning, metropolitan infrastructure policy, emergency preparedness, and strategic infrastructure utilization in Indonesia and comparable urban environments (Creswell & Poth, 2018; Lincoln & Guba, 1985; Patton, 2015).

Future research should operationalize the GDLR-G framework through geospatial mapping, network vulnerability analysis, scenario-based logistics simulation, and comparative studies across other strategic cities. Such research would help determine which nodes and corridors require the highest priority, how redundancy investments should be sequenced, and how civil-military governance arrangements can be tested under realistic crisis scenarios. For Jakarta, the immediate policy priority is to institutionalize geodefense as a planning logic that links space,

infrastructure, policy, and defense readiness in one integrated system (Linkov & Trump, 2019; NATO, 2024; OECD, 2019).

7. Policy Design Implications and Implementation Pathway

The GDLR-G framework is not intended to remain at the level of an abstract conceptual model. Its policy value depends on whether it can be translated into implementable instruments for Jakarta's metropolitan governance environment. The first implementation requirement is a formal criticality inventory that classifies infrastructure according to defense logistics relevance. This inventory should not merely list assets. It should identify each asset's operational role, spatial position, interdependency, alternative routes, controlling authority, normal utilization pattern, crisis utilization potential, and dependency on energy, communications, cyber systems, and human resources. Such an inventory would allow planners to distinguish between infrastructure that is important in an economic sense and infrastructure that is decisive for defense logistics continuity under stress (Head, 2023; Rittel & Webber, 1973).

The second requirement is the creation of a Defense Infrastructure Mapping System, or DIMS, as the operational expression of geodefense mapping. DIMS should combine geospatial layers on ports, airports, roads, railways, government centers, logistics depots, fuel distribution, power supply, telecommunications, water systems, hospitals, emergency facilities, and evacuation corridors. The value of DIMS is not simply cartographic. Its primary value is decision support. During normal conditions, it can be used to assess vulnerabilities and plan redundancy. During alert conditions, it can identify which routes and facilities must be protected or prepared. During emergency conditions, it can support prioritization, rerouting, and mobilization decisions. During recovery, it can support after-action review and resilience improvement (Cybersecurity and Infrastructure Security Agency, 2024; OECD, 2019).

The third requirement is a policy alignment matrix. The NVivo findings showed that policy constraints were among the most prominent themes, which means that the governance problem cannot be solved only through technical mapping. Existing planning documents, infrastructure regulations, defense policies, disaster management arrangements, and local development priorities need to be reviewed against a common defense logistics resilience checklist. The matrix should ask whether each policy instrument identifies critical nodes, recognizes dual-use infrastructure potential, defines crisis authority, includes civil-military coordination mechanisms, provides emergency priority rules, and requires periodic exercises. This would help convert broad policy principles into operationally relevant alignment criteria (Ansell & Gash, 2008; Head & Alford, 2015; OECD, 2019).

The fourth requirement is a standing geo-defense governance forum. Many coordination structures become active only after a crisis has already occurred. The logic of GDLR-G is different: coordination must be routinized before disruption. The forum should include representatives from defense institutions, the Jakarta provincial government, transportation authorities, port and airport operators, energy providers, telecommunications providers, cyber security institutions, police, disaster management agencies, state-owned enterprises, and selected private operators. Its tasks should include updating the criticality inventory, validating geodefense maps, conducting scenario planning, reviewing policy alignment, agreeing emergency priorities, and monitoring readiness exercise outcomes (Ansell & Gash, 2008; Government of Indonesia, 2019, 2021; NATO, 2024).

The fifth requirement is an exercise-based readiness cycle. The NVivo node on readiness exercises had a smaller coded-reference count than field vulnerability, policy constraints, or functional integration, but it is operationally indispensable. A governance model that is not exercised will remain fragile. Jakarta's defense logistics readiness should therefore be tested through tabletop exercises, command-post exercises, field simulations, and interagency drills. These exercises should use scenarios such as port disruption, fuel supply interruption, cyberattack on logistics data systems, flooding that affects strategic corridors, disruption to mass transportation, and simultaneous public-order and logistics pressures. The objective is not only to test technical capacity but to test decision authority, information flow, interagency trust, and public-service continuity (United Nations Office for Disaster Risk Reduction, 2015; U.S. Department of Defense, 2022).

The sixth requirement is a phased implementation strategy. In the short term, Jakarta can begin with document review, critical-node identification, and the establishment of an interagency working group. In the medium term, the government can develop DIMS, formulate policy alignment matrices, and design crisis priority protocols. In the long term, the framework should be institutionalized into metropolitan development planning, defense resource management, critical infrastructure protection policy, and recurring multi-actor exercises. This phased logic is important because a full geodefense governance system cannot be built instantly. It requires legal clarity, data integration, organizational trust, technical capacity, and sustained political commitment (Head, 2023; OECD, 2019).

The seventh requirement concerns indicators. A model becomes governable only when its implementation can be monitored. Potential indicators include the percentage of critical nodes mapped in DIMS, the number of infrastructure sectors included in the policy alignment matrix, the number of agencies participating in the standing forum, the existence of crisis priority protocols, the frequency of joint exercises, mean time to operational coordination during simulations, availability of alternative logistics routes, and the proportion of critical facilities with tested redundancy plans. These indicators would allow the GDLR-G framework to be evaluated as a living governance system rather than as a one-time academic model (Cybersecurity and Infrastructure Security Agency, 2024; Linkov & Trump, 2019).

Finally, implementation must address institutional sensitivity. Defense logistics, infrastructure vulnerability, and critical-node mapping involve information that may be operationally sensitive. Therefore, GDLR-G should include data classification rules, access control, and layered information-sharing protocols. Not every actor needs access to the same level of detail. Public-facing policy can describe the need for resilience and coordination, while restricted operational layers can contain sensitive route, facility, and vulnerability data. This balance is essential so that geodefense governance strengthens resilience without increasing security exposure. In this sense, the model requires both openness for coordination and discipline for information protection (NATO, 2022, 2024; U.S. Department of Defense, 2022).

8. Manuscript Contribution and Practical Relevance

The manuscript is positioned for international readership by linking an Indonesia-based empirical case to broader debates in urban resilience, critical infrastructure governance, defense logistics, and qualitative policy methodology. Its originality lies in the combination of geodefense and NVivo-assisted model construction. The following table summarizes the main contribution claims that can be refined further according to the target journal scope (Allsop et al., 2022; Graham, 2010; Linkov & Trump, 2019; OECD, 2019).

Table 5. Summary of article contribution claims. Source: Processed by the author using NVivo 15, 2026.

Contribution area	Specific contribution
Theory	Integrates geodefense, defense logistics, urban resilience, and collaborative governance into the GDLR-G framework
Method	Demonstrates a transparent pathway from NVivo coding, hierarchy visualization, and thematic interpretation to model construction
Empirical case	Provides Jakarta-based evidence on strategic infrastructure vulnerability, policy fragmentation, and civil-military integration needs
Policy	Offers a five-pillar governance framework for mapping, prioritizing, coordinating, and exercising defense logistics infrastructure resilience
Future research	Opens opportunities for geospatial risk scoring, network analysis, scenario simulation, and comparative metropolitan studies

Acknowledgements

The author acknowledges the academic and institutional support that enabled the development of the underlying dissertation research. Any errors in interpretation remain the responsibility of the author.

Funding

No external funding is declared in this manuscript draft.

Data Availability Statement

The qualitative data supporting the article consist of interview transcripts, policy documents, and NVivo project outputs generated for the doctoral research. Access to raw interview data is restricted to protect confidentiality and institutional sensitivity.

Conflict of Interest

The author declares no conflict of interest.

References

1. Ackoff, R. L. (1971). Towards a system of systems concepts. Management Science, 17(11), 661-671. https://doi.org/10.1287/mnsc.17.11.661
2. Alberts, D. S., & Hayes, R. E. (2003). Power to the edge: Command and control in the information age. CCRP Publication Series.
3. Allsop, D. B., Chelladurai, J. M., Kimball, E. R., Marks, L. D., & Hendricks, J. J. (2022). Qualitative methods with NVivo software: A practical guide for analyzing qualitative data. Psych, 4(2), 142-159. https://doi.org/10.3390/psych4020013
4. Amin, M. (2002). Toward secure and resilient interdependent infrastructures. Journal of Infrastructure Systems, 8(3), 67-75.
5. Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. Journal of Public Administration Research and Theory, 18(4), 543-571. https://doi.org/10.1093/jopart/mum032
6. Bazeley, P., & Jackson, K. (2013). Qualitative data analysis with NVivo (2nd ed.). SAGE.
7. Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27-40. https://doi.org/10.3316/QRJ0902027
8. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa
9. Braun, V., & Clarke, V. (2021). Thematic analysis: A practical guide. SAGE.
10. Checkland, P. (1981). Systems thinking, systems practice. Wiley.
11. Checkland, P., & Scholes, J. (1990). Soft systems methodology in action. Wiley.
12. Cybersecurity and Infrastructure Security Agency. (2019). A guide to critical infrastructure security and resilience. U.S. Department of Homeland Security.
13. Cybersecurity and Infrastructure Security Agency. (2024). Infrastructure resilience planning framework. U.S. Department of Homeland Security.
14. Clausewitz, C. von. (1976). On war (M. Howard & P. Paret, Eds. and Trans.). Princeton University Press.
15. Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE.
16. Denzin, N. K. (2012). Triangulation 2.0. Journal of Mixed Methods Research, 6(2), 80-88. https://doi.org/10.1177/1558689812437186
17. European Commission. (2022). Action plan on military mobility 2.0. European Commission.
18. Graham, S. (2010). Cities under siege: The new military urbanism. Verso.
19. Graham, S., & Marvin, S. (2001). Splintering urbanism: Networked infrastructures, technological mobilities and the urban condition. Routledge.
20. Government of Indonesia. (2002). Law No. 3 of 2002 concerning national defense.
21. Government of Indonesia. (2019). Law No. 23 of 2019 concerning management of national resources for national defense.
22. Government of Indonesia. (2021). Government Regulation No. 3 of 2021 concerning implementation of Law No. 23 of 2019 on management of national resources for national defense.
23. Head, B. W. (2023). Wicked problems in public policy: Understanding and responding to complex challenges. Palgrave Macmillan.
24. Head, B. W., & Alford, J. (2015). Wicked problems: Implications for public policy and management. Administration & Society, 47(6), 711-739. https://doi.org/10.1177/0095399713481601
25. Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies.
26. Holling, C. S. (1973). Resilience and stability of ecological systems. Annual Review of Ecology and Systematics, 4, 1-23. https://doi.org/10.1146/annurev.es.04.110173.000245
27. Kaldor, M. (2012). New and old wars: Organized violence in a global era (3rd ed.). Stanford University Press.
28. Kilcullen, D. (2013). Out of the mountains: The coming age of the urban guerrilla. Oxford University Press.
29. Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. SAGE.
30. Linkov, I., & Trump, B. D. (2019). The science and practice of resilience. Springer.
31. Meerow, S., Newell, J. P., & Stults, M. (2016). Defining urban resilience: A review. Landscape and Urban Planning, 147, 38-49. https://doi.org/10.1016/j.landurbplan.2015.11.011
32. Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). Qualitative data analysis: A methods sourcebook (3rd ed.). SAGE.
33. Ministry of Defence of the Republic of Indonesia. (2015). Indonesian defense white paper. Ministry of Defence.
34. Moustakas, C. (1994). Phenomenological research methods. SAGE.
35. NATO. (2022). NATO 2022 strategic concept. North Atlantic Treaty Organization.
36. NATO. (2024). Resilience, civil preparedness and Article 3. North Atlantic Treaty Organization.
37. OECD. (2019). Good governance for critical infrastructure resilience. OECD Publishing. https://doi.org/10.1787/02f0e5a0-en
38. Patton, M. Q. (2015). Qualitative research and evaluation methods (4th ed.). SAGE.

39. Rittel, H. W. J., & Webber, M. M. (1973). Dilemmas in a general theory of planning. Policy Sciences, 4, 155-169. https://doi.org/10.1007/BF01405730
40. Rodin, J. (2014). The resilience dividend: Being strong in a world where things go wrong. PublicAffairs.
41. Saldaña, J. (2021). The coding manual for qualitative researchers (4th ed.). SAGE.
42. Silver, C., & Lewins, A. (2014). Using software in qualitative research: A step-by-step guide (2nd ed.). SAGE.
43. Strauss, A., & Corbin, J. (1998). Basics of qualitative research: Techniques and procedures for developing grounded theory (2nd ed.). SAGE.
44. UN-Habitat. (2022). World cities report 2022: Envisaging the future of cities. United Nations Human Settlements Programme.
45. United Nations Office for Disaster Risk Reduction. (2015). Sendai framework for disaster risk reduction 2015-2030. United Nations.
46. U.S. Department of Defense. (2022). National defense strategy of the United States of America. U.S. Department of Defense.